NAVAL WAR COLLEGE
Newport, RI

The Challenge of Netwar for the Operational Commander

by

James A. Poole

LCDR, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: James A. Poole

6 March 1996

Paper Directed by Captain D. Watson
Chairman, Joint Military Operations Department

Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): The Challenge of Netwar for the Operational Commander (Unclassified)	
9. Personal Authors: LCDR James Andrew Poole, USN	
10.Type of Report: FINAL	11. Date of Report: 6 March 1996
12.Page Count: 29	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Netwar, Information Warfare, computer networks, operational, defense, offense, command & control, information.	

15.Abstract: The threat of intrusions to U.S. domestic and military infrastructure and information systems is very real and may affect our national security now and in the future. Information has become a new center of gravity that must be protected. Netwar is one tool of Information Warfare that the operational commander can use in defensive and offensive operations to gain information dominance. Netwar targets military or civilian non-weapons computer networks to gain a military advantage while it protects one's own systems from attack. With an overview of Netwar concepts, this paper explores the benefits of Netwar for the commander, the defensive and offensive decisions that must be made, and some prescriptions for the future that will enable the commander to fight and win conflicts effectively in the twenty-first century.

16.Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17.Abstract Security Classification: UNCLASSIFIED	
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19.Telephone: 841-[redacted]6461	20.Office Symbol: C

Security Classification of This Page Unclassified

ABSTRACT

The threat of intrusions to U.S. domestic and military infrastructure and information systems is very real and may affect our national security now and in the future. Information has become a new center of gravity that must be protected. Netwar is one tool of Information Warfare that the operational commander can use in defensive and offensive operations to gain information dominance. Netwar targets military or civilian non-weapons computer networks to gain a military advantage while it protects one's own systems from attack. With an overview of Netwar concepts, this paper explores the benefits of Netwar for the commander, the defensive and offensive decisions that must be made, and some prescriptions for the future that will enable the commander to fight and win conflicts effectively in the twenty-first century.

The Challenge of Netwar for the Operational Commander

Table of Contents

The Challenge of Netwar for the Operational Commander

I. Introduction

> "The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data. It's all just electrons. ...There's a *war* out there...A *world* war. And it's not about who's got the most bullets. It's about *who controls the information*." [1]

The United States is in the midst of a tremendous transformation of world history that is creating a new social, economic, and political order. The explosion of computer technology and the desire for global interconnectedness have created an Information Revolution linking nations, companies, and peoples. This technological sophistication has provided a means by which to achieve superiority as an economic and military power. Our increasing reliance on this technology for the efficient exchange of personal, corporate, and government information is not without risk. Consequently, information is now a "strategic asset worthy of conquest and destruction." [2] The threat of intrusions to U.S. domestic and military infrastructure and information systems is very real and has the potential to affect the national security of the United States now and into the twenty-first century. "Information Warfare is coming. For some, it has already arrived." [3]

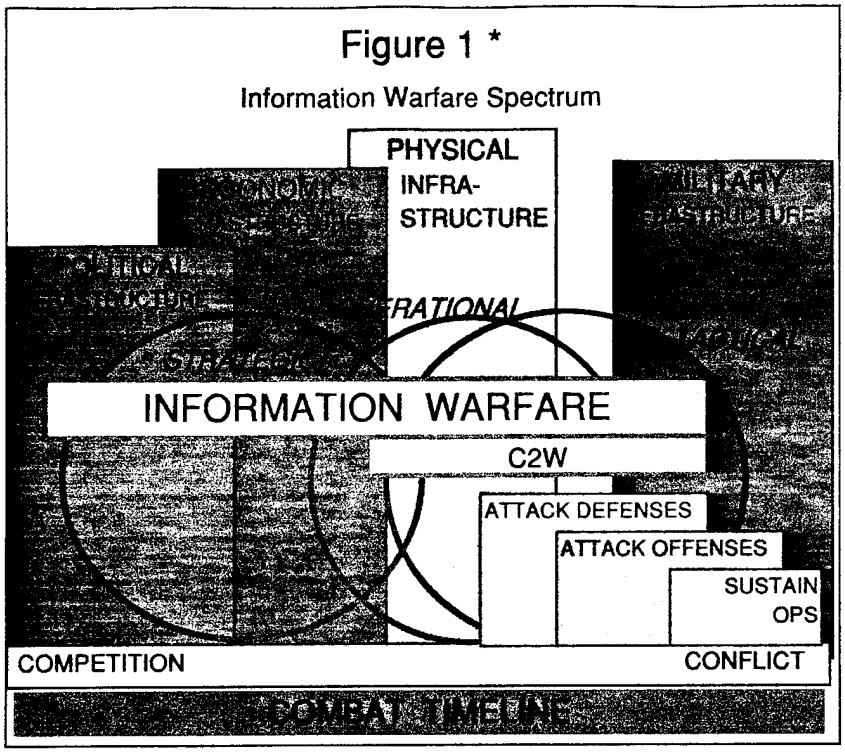
This new Information Age of technology is impacting every facet of our daily lives, and it is affecting how the military conducts war today and in the future. Network communications systems have become increasingly vital for our civilian and military communities. As a result, Information Warfare (IW) will continue to develop into an important weapon for today's operational commander who depends on the processing of large volumes of information through the use of various networks and databases. Network warfare, or "Netwar," is one aspect of IW that the commander must be able to use effectively in the twenty-first century. Today's commander must anticipate, plan, and integrate Netwar into his war-fighting arsenal. The commander must understand

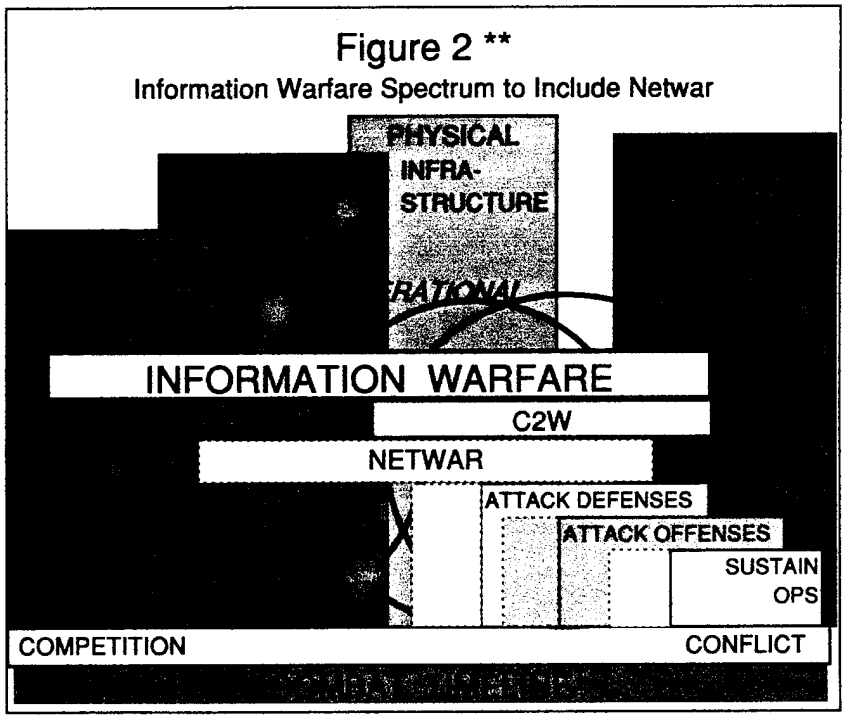
Netwar as it relates to operational design, successfully secure his own friendly information systems, and work Netwar offensively against a variety of potential adversaries. This paper explores the benefits Netwar holds for the commander and the defensive and offensive decisions that must be considered as he strives to successfully manipulate information systems to his advantage while thwarting those of his adversary. Ultimately, it may be the operational commander's understanding of the strengths and limitations of Netwar and his application of that knowledge that will determine his success.

II. Information Concepts

"Information is the only asset that can be in two places at the same time."
--- Charles Robertello [4]

Information is, to a large extent, synonymous with knowledge. It includes "knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium." [5] Today, information is increasingly becoming "the currency of true military and economic power." [6] Information must be protected; as a result, the military has recently begun to define Information Warfare. One such definition describes Information Warfare (IW) as "...actions taken to achieve information superiority in support of national strategy by affecting adversary information systems while leveraging and defending our own information and systems." [7] As shown in Figure 1, the concept of Information Warfare transcends all levels of warfare (strategic, operational, and tactical) and includes a wealth of concepts.[8] At the strategic level, IW may involve political, military, economic, and social targets. It involves both offensive capabilities as well as defensive vulnerabilities. The goal of IW is to achieve information superiority, or "information dominance." This dominance is viewed as a key to a decisive advantage over an adversary both in technological and economic competition and in conflict.





* Adapted from the figure in Gerald Burnette's "Information: The Battlefield of the Future," Surface Warfare, July/August 1995, p. 8.

** Created by the author to illustrate a conception of Netwar within the Information Warfare Spectrum.

Much has been written about one subset of Information Warfare: Command and Control Warfare (C2W). While its definition too, is still evolving,[9] C2W is described as "the military strategy that implements IW on the battlefield and integrates physical destruction." [10] Generally speaking, while IW is an all-inclusive term describing political, economic, and military aspects, C2W deals primarily with Information Warfare's military aspects. [11]

A new subset of Information Warfare has been recently termed "Netwar." [12] Like C2W, it too involves executing offensive and defensive operations; Netwar involves conducting these operations on military or civilian non-weapons computer networks to gain a military advantage.[13] Netwars could be largely "non-military," but they could have dimensions that overlap into military warfare. Looking at Figure 2, one can see that Netwar (See the dotted lines) represents a "new entry in the spectrum of conflict that spans economic, political, social, as well as military forms of war." [14] Netwars specifically target information and communications systems. The weapons of Netwar are extensive. They range from software devices such as viruses, trap doors, sniffers, worms, and data interception techniques to hardware devices that use High Power Microwaves (HPM), Electromagnetic Pulse (EMP), Van Eck radiation, HERF Guns and active wiretapping. Readily available today, these hard/soft kill, overt/covert weapons can be used independently or in any combination to help achieve the commander's or adversaries' warfare goals. Netwar, whether described as a new subset of IW or a future extension of the evolving concept of C2W, is an important concept that must be understood by the operational commander.

III. Netwar and the Commander

> "We have crossed the threshold. We have to change fast to be able to fight and win in the information age. It's time to be proactive and keep the Navy ahead of the information bow wave. It is clear to me that information has become a major factor in warfare and will grow in importance in the next century. I challenge you all to join me as we redefine how wars are fought and won." ---Admiral J.M. Boorda[15]

Revolution in Military Affairs. In this Information Age, knowledge has now become synonymous with power. The technology that pervades nearly every aspect of our daily lives has created a Revolution in Military Affairs that is changing and influencing military thinking and planning. Consequently, this change in modern warfare is being compared to the revolutions that brought about the mechanization of land forces and the development of airpower.

In the past, the United States relied heavily upon the use of conventional weapons, in conflicts typically centered around land and capital. Now, the trends in modern warfare pursue a new form of capital: information. Information dominance in competition and in conflict may bring national power.[16] Because information brings the promise of power, it is fast becoming a new center of gravity; one who controls that center of gravity, in essence, holds the power. As we increasingly interact through networks that link civilian and military information systems together, the more likely it is that conflicts will arise on those systems. Our extensive reliance on these network systems increases our vulnerability to attack by our adversaries. U.S. information systems are attacked daily;[17] it is only a matter of time before conflicts or warfare will take place on these same vital network, communication, and data systems.

In warfare, where the goal is to win in a conflict with one's adversary, the commander must choose the weapons that give him an advantage over that adversary. In the fight for information dominance, the use of computers, technology, and networks of Netwar can give the commander that advantage. The commander must anticipate the operational context of Netwar so that he can maximize its impact on potential courses of action.

Netwar in Context. For the commander, the Information Revolution directly influences the operational context from which he must work in conflict situations. Pursuing information dominance, the commander may opt not to annihilate his adversary, but

rather to "paralyze" or "blind" him in battle, or he may decide to do both. Using computers and network systems as his tools, he will target his adversary's command and control systems, aiming to slow down his adversary, and to introduce uncertainty into the enemy's Observe, Orient, Decide, and Act (OODA) Loop. Information systems will allow the commander to share common situational awareness with his forces on an extended battlefield in near real time, enabling him to make adjustments quickly and efficiently, as necessary. He can plan, synchronize, and execute complex maneuvers.

The weapons of Netwar allow a flexibility in the degree of lethality that can be imposed on an adversary's center of gravity. Executed with precision, Netwar weapons can reduce collateral damage while at the same time, increase the destructiveness of a strike. Netwar could be used to put pressure on an adversary to change his behavior and avert further conflict. It may also be used by the commander to help control the possible escalation of a conflict.

The Information Age is transforming military operations by providing commanders with information that is "unprecedented in quantity and quality." [18] The increased data can provide the commander with a superior understanding of the conflict situation in a short period of time so that he can make the appropriate decisions quickly. Ultimately, this information dominance will speed up the tempo of operations and outpace the enemy's decision-making cycle. The commander's ability to gain information and interpret it more carefully and quickly than his adversary is the key to winning on the Netwar battlefield. [19]

Intelligence, Not Just Information. Modern warfare forces the commander to make decisions at a high tempo, often under conditions of great uncertainty. As the quantity of data and the role of the commander both increase, it is very likely the precision and timeliness of the information will decrease.[20] Mistakes such as the Iranian Airbus shoot-down by the *U.S.S. Vincennes (CG 49)* can happen. What

becomes increasingly vital to Netwar operations is not *more* data, but *quality* data that has been interpreted into *quality intelligence*. Effective decision-making can only take place when there has been a reduction of uncertainty in a timely fashion. That uncertainty can be reduced by commanders who properly direct intelligence efforts so that information about the enemy is as complete and reliable as possible.[21] One cannot collect *all* intelligence, as that would cause "information overload" and ultimately slow down the commander's OODA loop.

No data system today can meet the insatiable demand for information that can take place in a conflict. The commander needs to understand intelligence systems capabilities and their limitations,[22] direct the gathering of intelligence data in an ongoing fashion in conflict and in peacetime, and decide what is needed and who should get what. There will have to be "a certain amount of appetite suppression." [23]

IV. Netwar in a Defensive Posture

> "It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible." ---Sun Tsu [24]

The Goals of Netwar. With today's upwardly spiraling technology, there is no such thing as a "secure" network system. Almost every file that is stored magnetically, transmitted over a wireline, radio or fiber-optic link is subject to interception by an adversary.[25] Nearly every component of the U.S. military and its supporting infrastructure is highly dependent on its information and information systems. [26] The United States, the most technologically advanced country in the world, is *without question the most vulnerable* to Netwar.

One goal of Netwar is to provide the commander with the information necessary to seize and maintain information dominance over his adversary. That data is collected through the use of friendly network and communications systems. However, the

commander must be able to *trust* incoming information and be assured that it has not been contaminated or corrupted in any way. Without the certainty that comes from trusted information, the commander cannot make intelligent, effective operational decisions during a conflict or in peacetime.

The most crucial aspect of Netwar is the ability of the U.S. to defend its network infrastructures from intrusion and compromise by potential adversaries. With tens of thousands of computers all interconnected, the damage that can be inflicted by a single computer or a computer-controlled network is incredible. In 1994, the Joint Security Commission called the U.S. vulnerability to Information War "the major security challenge of this decade and possibly the next century." [27] The United States must be able to defend its defense network infrastructure, otherwise, military readiness will be compromised.

Defensive Netwar measures must be taken on a *continual* basis in peacetime and in conflict. The Pentagon alone is probed electronically by outsiders "close to 500 times a day." [28] We must expect there will be continuous, deliberate attempts to destroy or damage our information infrastructures in the future.[29] The commander must seriously assess the vulnerabilities of the network infrastructures in his area of responsibility, evaluate the possible actions of potential adversaries, and make informed, prioritized decisions to take the necessary defensive actions to secure his network systems.

Assessment of Vulnerabilities. The commander must become familiar with the particular vulnerabilities of his systems. He may choose to do so by contacting the appropriate Information Warfare authorities[30] for updated assessment of current vulnerabilities. Assessment must be made on an ongoing basis through purposeful attempts to infiltrate one's own systems.

Netwar is particularly difficult to assess and defend against because, unlike attacks using conventional weapons, it can be difficult to know when one has been attacked on a network. Although the Department of Defense (DoD) does not openly discuss computer security breaches, one Defense agency conducted its own mock attacks on more than 8,000 DoD computers over the last two years. The Defense Information Systems Agency's (DISA) team was able to break into more than 88% of the computers. Even more alarming, less than 5% (of the 7,860 systems penetrated) realized they had been attacked, and *only 5% of those* reported the incidents to authorities. [31]

It would be an extremely costly and lengthy process to provide widespread protection of civil and military infrastructures to make them more robust against degradation. [32] We cannot defend against *all* vulnerabilities to a network system. In light of that fact, it is important that the commander take inventory of each known vulnerability to the systems in his area of responsibility and assess the *value* of the vulnerable information. The information that is most critical to national security would be the most vital information to protect, while information whose corruption or interruption would not compromise national security would fall lower on the list of priorities. Through critical assessment of his vulnerabilities, the commander takes the first step in prioritizing his information assurance needs. Only then can he begin to meet the most crucial defensive Netwar needs of his theater.

The Threat. The present vulnerabilities of the United States to Netwar are of greater concern right now than the known threats. However, in the coming years, the number of nations and individuals with the capability to access and damage our systems should grow substantially.[33] The operational commander must carefully and continually evaluate the potential for any adversary to attack our systems. He must become very

familiar with who these adversaries are or *could* be, what their capabilities are, and what their intentions are as well.

With the shrinking price of high-performance computers, coupled with the proliferation of high-speed digital communications, the threat of Netwar rises, and more and more foreign governments and non-government groups and individuals become a threat to U.S security.[34] In the highly unpredictable post Cold War age in which we live, the commander cannot make assumptions as to who his adversaries will be. Tomorrow's enemy may or may not be a nation-state. We may find ourselves attacked by adversaries such as clans, terrorists, ethnic factions, religious groups, or drug cartels.

The commander cannot assess an adversary strictly by measuring capability. In a sense, capability is a given. Much of the technology that is needed is widely available at a low cost. Even an adversary who does not have the capability to wreak havoc can have access to state-of-the-art knowledge and equipment by finding a "Hacker for Hire" for the right price. The commander must shift his attention to the motivations or intentions of a potential adversary. Very often, careful consideration of those intentions will give a better defense barometric reading than a measure of capability alone. If a potential U.S. target is *vulnerable* and is *vital* to our national interests and an adversary has the *capability and intention* to disrupt that particular target, then the commander must work to protect that system.

The Defense. The operational commander has four defensive approaches to thwart potential adversaries: *prevention, detection, limitation, and recovery.*[35] While prevention may be the most attractive option of all, it may not be the most feasible for all systems. The commander should consider a cost-benefit analysis to determine what action is the most appropriate for a given system.[36]

- ***Prevention***. Successful prevention measures leave the intruder completely blocked from a system. Computer facilities must be made secure from intrusion. This can be done by ensuring the physical design of those structures and the computer hardware itself are protected so that electronic emissions cannot be intercepted by an adversary. Encryption software and hardware should be used on the most crucial information. Security personnel must receive ongoing training and be monitored to ensure that they follow through on all necessary security measures. A majority of security breaches could be prevented if personnel enforced the security guidelines already in place.[37]

- ***Detection*** of an intruder is a very difficult task. DISA has estimated that only 5% of all attacks on military systems through the Internet are detected.[38] Viruses and other passive intrusions may lay dormant for years without detection. Because it is so difficult to know if one has been attacked, one cannot rely on detection systems alone for defense. The commander must maintain the integrity of his computer systems by running comparison checks with other systems and use passive detection devices such as sniffers to protect systems from being purposefully overloaded by an adversary.

- ***Limitation***. Very often, computer networks are protected by limiting access to information systems through various user ID and firewall procedures. Because no system is 100% protected, these limitation procedures may give a false sense of security to those who rely on them. It is only a matter of time and persistence before an intruder will get through. As Douglas Waller, a *Time* magazine journalist explains, "The toughest Pentagon computer to crack is the first one; once inside, nearly 90% of the other computers linked to the first computer will recognize the intruder as a legitimate user." [39] Obviously, extremely sensitive information must be protected by other means if at all possible.

♦ ***Recovery.*** The commander must guard against attack by planning and preparing for a possible strike against vital network systems. These systems must be recovered as quickly as possible, so that military effectiveness and readiness are not compromised. Backup systems must be maintained so that systems can be restored to their previous working potential.

Defensive measures must be taken on a continual basis to ensure the certainty of our information systems. We cannot become complacent. As computer capacity continues to double every two years and will probably continue to do so for the next few decades,[40] the speed and complexity of computer systems will increase at an astronomical rate. It will become increasingly difficult to defend our information systems of today against the technology of tomorrow. We must endeavor to always stay a few steps ahead of our adversaries.

V. Offensive Use of Netwar

> "In order to win victory we must try our best to seal the eyes and ears of the enemy, making him blind and deaf, and to create confusion in the minds of enemy commanders, driving them insane." ---Mao Tse-Tung [41]

Ideally, in peacetime or in conflict, the commander would seek to keep his adversaries from being able to gain knowledge of U.S. forces, or learn of U.S. intentions. If engaged in a conflict situation, the commander should strive to thwart the enemy leader's efforts to communicate among his own units.[42] If successful, the commander will be able to work comfortably in his OODA Loop while disrupting the decision-making cycle of his opponent. This will force the enemy to lose the initiative, and cause the enemy to resort to a reactive mode of operation. [43]

Before the commander can take such actions effectively, he must have a clear understanding of the overall mission. Ongoing peacetime planning must involve the development and maintenance of offensive Netwar capabilities and resources.

Through continuous peacetime activities, the Netwar commander will be able to *observe* the situation, *orient* available forces to meet the perceived threat, *decide* a course of action to counter the threat, and then, in conflict, *act* in a quick and decisive manner.

Observe. The commander must have an understanding of his adversary's (or potential adversaries') Netwar vulnerabilities long before the time of conflict, and he should focus on those adversaries most likely to attack. The commander will need to know who the adversary is, what makes him "tick," where his vulnerabilities are, and what it may take to weaken his will. An effective commander will know the last step before he takes the first.[44] Measures should reflect war termination goals for post war reconstruction. It is easier to rebuild an adversary's disabled system vice a destroyed one. The commander will devise a course of action that clearly states the Netwar objectives and not lose sight of those goals in the heat of conflict. Although he will have the choice of a full range of weapons of attack, he will choose those that have the potential to deliver the most *effective* blow in the most efficient manner possible. The most effective blow may be quick and decisive, or may just cause confusion for the enemy for a short time. Properly executed Netwar can bring an adversary to his knees by hitting him swiftly in his most vulnerable network systems, without necessarily physically destroying those systems. Or, Netwar can slowly degrade an adversary's information systems to the point that the enemy no longer trusts the information on those systems.

Properly directed intelligence efforts will assist the commander as he develops a situational awareness of the adversarial conflict. Understanding of the enemy's culture and his perspective as well as his military infrastructure and information systems architecture will facilitate the commander in his efforts to select appropriate Netwar targets of vulnerability and nodes of attack.

Orient. The orientation surrounding target selection is perhaps the most challenging dimension of offensive Netwar for the operational commander. The decisions regarding the selection and prioritization of targets will involve political, cultural, and military decisions. The identification of an adversary's centers of gravity and the assessment of the consequences of their neutralization must be as precise as possible so that the appropriate weapon(s) can be chosen for the job.[45]

Because Netwar involves information systems and infrastructures, careful study of the adversary's systems during peacetime will yield the most effective results during a conflict. Intelligence-gathering operations would involve the collection of information regarding the information infrastructure of the adversary, the important links within those systems, and how those systems depend upon each other.[46]

First, one must determine which systems are the most important to the adversary, as well as which systems could pose a threat to our forces' systems we may choose to employ. The commander and his planners should determine which links in the system are *susceptible* to degradation, *accessible* to friendly forces, and *feasible* to attack. If these links or "nodes" in a system meet these three criteria, then they are considered "vulnerable." [47] Each vulnerable node must then be evaluated to determine how critical it is: that is, is an attack on the node by the commander necessary to meet the overall objectives or goals of the conflict? If these vulnerable nodes meet these goals, then the commander must determine the priority level of each of these targets.

Decide. The kinds of targets that may be compromised are numerous. The decision regarding what to target is dependent upon the nature of the conflict. One may decide to target a physical computer network, a computer support structure, or a particular product of a network. It may be that the targeting priority against an adversary would resemble the one employed in the air battle against Iraq. Col. John A. Warden, III of the Air Staff Plans Directorate developed a schematic that rank-ordered

the components of the adversary as follows: leadership, material essentials, infrastructure, the people, and the military.[48] Netwar would concentrate on those infrastructures and information systems, both military and civilian, that would cut off the adversary leadership from its supporting infrastructure and deny or disrupt those systems.

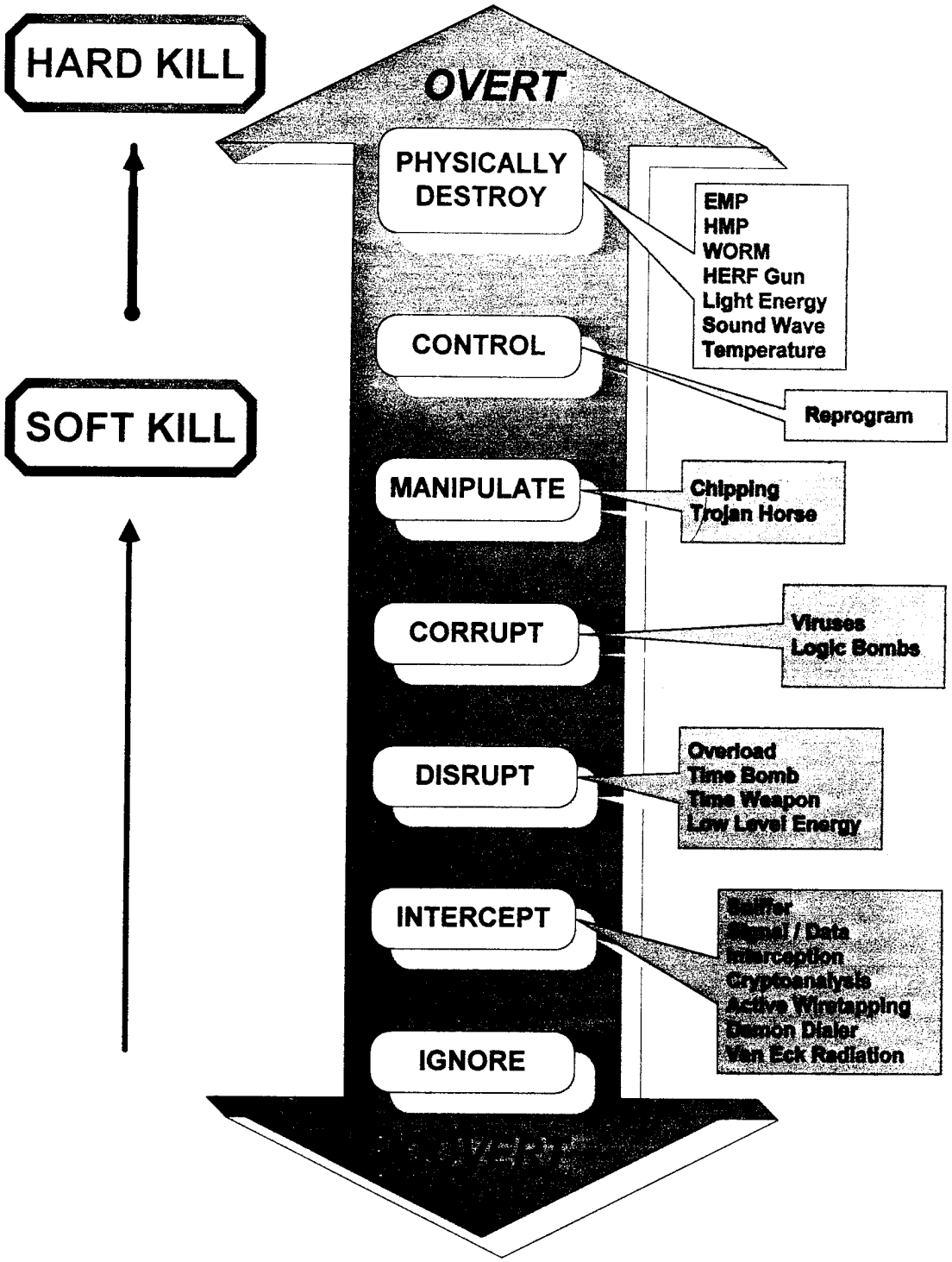
The method of attack against a target can be overt or covert. There are a number of modes of attack that can be employed and they fall along a continuum of destruction (See Figure 3). In Netwar, the commander can choose to ignore, intercept, disrupt, corrupt, manipulate, control, or physically destroy the network systems or products of those systems.[49] The decision of which mode to utilize on which system will not be made by the operational commander alone. The National Command Authority would have to approve some types of non-traditional military operations (economic and political targets / networks) before they could be pursued.

Act. When it is time to act upon the adversary, the preparedness of the operational commander will become most evident. Netwar planning and operations are multi-dimensional, involving the coordination of diverse forces to strike most effectively at the weakest and most decisive points. Timing can be paramount: strike too soon, and the adversary may be able to recover. Strike too late and the action is useless.

The final decision to act upon targets could be influenced by political, moral, and practical issues as well. Netwar does not take place in a vacuum. It can affect a conflict across a number of social and moral issues. In this day and age of instant media coverage, one cannot ignore the political ramifications of a decision to act upon a target that the American or international public may deem inappropriate or inhumane. In the future, Netwar may be used to prevent conflicts from escalating to the use of conventional forces. Some believe it may even replace conventional warfare as the non-lethal weapon of the future.

FIGURE 3

Modes of Netwar Attack and Examples



"The supreme excellence is not to win a hundred victories in a hundred battles. The supreme excellence is to subdue the armies of your enemies without even having to fight them." --- Sun Tsu [50]

VI. Recommendations and Final Thoughts

"The ultimate goal is simple: Give the battlefield commander access to all the information needed to win the war. And give it to him when he wants it, where he wants it, and how he wants it." --- General Colin L. Powell [51]

As the realities of the Revolution in Military Affairs merge with the realities of the post Cold War world, the U.S. military will need to make some organizational adjustments to keep pace in the years ahead.

While it is necessary to maintain separate IW communities within each of the armed services, it is imperative that continuous joint planning be undertaken to ensure the efficient coordination of all Netwar activities. The centralization of Netwar planning will guard against redundancy of information collection efforts and help to ensure the stealth of covert operations. In peacetime and in conflict, the coordination must be such that all communities are well aware of what each of the others is doing. The operational commander must decentralize Netwar at the execution level to maximize the flexibility of the field operations. In addition, the close working relationship required between the operational and intelligence communities necessitated in Netwar may require those specialties to merge in the future.

In this era of force downsizing, there is a planning dilemma as the operational commander must strike the appropriate balance between the need to invest in future technologies while maintaining an adequate force structure. While some argue we should be upgrading in our current capabilities, others argue that Netwar and Information Warfare will replace the need for conventional weapons. Further reductions in forces may require the consolidation of specialties and the training of troops who are capable of flexible multitasking.

The distinctions between civil and military communications and information systems will continue to blur. The traditional boundaries between what is the military domain and what is the non-military domain will increasingly fade. As a consequence of downsizing and the commercial drive of the civilian market, the military will grow dependent upon the private sector to support it through civilian technological innovation. The military is lagging as opposed to leading.[52] The operational commander must recognize the shift in civilian and military technology that is taking place and make strides towards a productive civil-military relationship in the future.

> "The only thing harder than getting a new idea into the military mind is to get an old one out." --- B. H. Liddell Hart[53]

ENDNOTES

[1] Sneakers, VHS, 2 hrs. 5 min., 1993, MCA Universal Home Video, Inc. Character Cosmos is speaking to Marty Bishop at the end of the movie.

[2] Winn Schwartau, Information Warfare: Chaos on the Superhighway (New York: Thunder Mountain Press, 1994), p. 13.

[3] Schwartau, p. 11.

[4] Charles Robertello, Information Security Expert, quoted in Schwartau, Information Warfare, p. 82.

[5] Planning Considerations for Defensive Information Warfare: Information Assurance (Arlington, VA: Defense Information System Agency, 1993), p. 54.

[6] Peter Grier, "Information Warfare, " Air Force Magazine, March 1995, p. 36.

[7] U.S. Dept. of Defense, Information Warfare, Draft, (Washington: April 1995), p. 2.

[8] Information Warfare includes actions to deny, exploit, corrupt, or destroy the adversary's information systems while protecting one's own.

[9] In Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, (Washington: 1995), p. GL-5, C2W is defined as "**command and control warfare**. The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict. Also called C2W, C2W is both offensive and defensive: **a. counter-C2** ---To prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. **b. C2 protection** --- To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

[10] Chairman of the Joint Chiefs of Staff, Command and Control Warfare, Memorandum of Policy No. 30, (Washington: 1993), p. 3.

[11] Wayne J. Rowe, Information Warfare: a Primer for Navy Personnel (Newport, RI: U.S. Naval War College, Strategic Research Department, 1995) p. 3.

[12] The term Netwar was first used by John Arquilla and David Ronfeldt from the International Policy Dept., RAND, Santa Monica, CA. Their paper, "Cyberwar is Coming!" is published in Comparative Strategy, April/June 1993, pp. 141-165.

[13] Stefan Eisen, Jr., "Netwar, It's Not Just for Hackers Anymore," Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995, p. 3.

[14] John Arquilla & David Ronfeldt, "Cyberwar is Coming!" Comparative Strategies, April/June 1993, p. 144.

[15] Admiral J. M. Boorda, Chief of Naval Operations, as quoted in Rowe, p. iii.

[16] "Information Dominance Edges Toward New Conflict Frontier," Signal, August 1994, p. 37.

[17] Winn Schwartau discusses the frequency and variety of attacks on U.S. information systems (government, corporate, and personal) throughout his book, Information Warfare: Chaos on the Superhighway.

[18] U.S. Dept. of the Air Force, Cornerstones of Information Warfare (Washington: 1995), p. 1.

[19] William B. Scott, " 'Information Warfare' Demands New Approach," Aviation Week & Space Technology, 13 March 1995, p. 86.

[20] Edward A. Smith, Jr., "Putting it Through the Right Window," U.S. Naval Institute Proceedings, June 1995, p. 40.

[21] As Smith explains in his article, p. 40, Effective collection of data and its transformation into intelligence is based on a solid understanding of what is being sought, and why. To collect everything is inefficient and would overload systems. Unless the intelligence collection is properly directed, then any attempt to gather less than everything risks missing the essential target.

[22] Ira C. Owens, "Army Intelligence Operations in Force XXI," Army, October 1994, p. 146.

[23] Peter Grier, "The Data Weapon," Government Executive, June 1992, p. 25.

[24] Sun Tsu as cited in Planning Considerations, page 3.

[25] Terry Metzgar, "Hostile Intercepts Aimed at Information Systems," National Defense, May/June 1993, p. 25.

[26] Planning Considerations, p. 8.

[27] Douglas Waller, "Onward Cyber Soldiers," Time, 21 August 1995, p. 40.

[28] Ibid., p. 44.

[29] Kerry A. Blount, "A Two-Component Strategy for Winning the Information War," Army, January, 1995, p.11.

[30] Organizations such as the National Security Agency (NSA), Defense Information Systems Agency (DISA), the Fleet Information Warfare Center (FIWC), and the Naval Information Warfare Activity (NIWA) would be helpful in this regard.

[31] Bob Brewin, "DISA Stings Uncover Computer Security Flaws," Federal Computer Week, 6 February 1995, p. 1.

[32] U.S. Dept. of Defense, Information Warfare, Draft, p. 3.

[33] Ibid.

[34] Bruce D. Berkowitz, "Warfare in the Information Age," Issues in Science & Technology, Fall 1995, p. 62.

[35] President's Council on Integrity and Efficiency, Computers: Crimes, Clues and Controls (Washington: 1986) p. 3.

[36] The commander will need to consider the costs of such procedures, measured in dollars, time, and restrictions in access. With the regeneration of computer systems over time, it may be *more* cost-effective and "worth the risk" *not* to protect older systems before it is time to replace them.

[37] Planning Considerations, p. 24.

[38] U.S. Dept. of Defense, Information Warfare, Draft, p. 3.

[39] Waller, p. 44.

[40] Gregory H. Canavan, "Changing Times Implode Defense Science Dynamics," Signal, September 1993, p. 50.

[41]Mao Tse-Tung from On the Protracted War (1938) quoted in Norman B. Hutcherson, "Command & Control Warfare--Putting Another Tool in the War-Fighter's Data Base," Published Research Paper, Maxwell Air Force Base, AL: Air University Press, September 1994, p. xiii.

[42] Jensen, p. 37.

[43] Hutcherson, p. 43.

[44] Carl von Clausewitz, On War , Michael Howard and Peter Paret eds. and trans., Princeton: Princeton University Press, 1976, p.263

[45] Smith, p. 39.

[46] Facsimile from Navy and Marine Corps Intelligence Training Center, "Nodal Analysis," Dam Neck, VA, 17 January 1996, p. 3.

[47] Ibid., p. 4.

[48] John Arquilla, "Strategic Implications of Information Dominance," Strategic Review, Summer 1994, p. 27.

[49] Eisen, p. 6.

[50] Sun Tsu as quoted in James Charlton, ed., The Military Quotation Book (New York: St. Martin's Press, 1990), p. 15.

[51]GEN Colin L. Powell, "Information-Age Warriors," Byte, July 1992, p. 370.

[52] Scott, p. 83.

[53] B.H. Liddell Hart as quoted in Charlton, p.65.

BIBLIOGRAPHY

Alexander, David. "Information Warfare and the Digitised Battlefield." Military Technology, September 1995, pp. 57-59+.

Anselmo, Joseph. "Information Needs to Grow as Budgets Shrink." Aviation Week & Space Technology, 7 November 1994, pp. 64-65.

"Army Views Combat Future in Digital Battlefield Tempo." Signal, May 1994, pp. 27-34.

Arquilla, John. "Strategic Implications of Information Dominance." Strategic Review, Summer 1994, pp. 24-30.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" Comparative Strategy, April/June 1993, pp. 141-165.

Berkowitz, Bruce D. "Warfare in the Information Age." Issues in Science & Technology, Fall 1995, pp. 59-66.

Blount, Kerry A. "A Two-Component Strategy for Winning the Information War." Army, January 1995, pp. 10-11.

Brewin, Bob and Elizabeth Sikorovsky. "DISA Stings Uncover Computer Security Flaws." Federal Computer Week, 6 February 1995, pp. 1, 45.

Bunker, Robert J. "The Tofflerian Paradox." Military Review, May/June 1995, pp. 99-102.

Burnette, Gerald. "Information: The Battlefield of the Future." Surface Warfare, July/August 1995, pp. 8-9.

Busey, James B. "Information Superiority Dashes Thorny Power Projection Issues." Signal, November 1994, p. 13.

Busey, James B. "Information Warfare Calculus Mandates Protective Actions." Signal, October 1994, p. 15.

Campen, Alan D. "Information Warfare is Rife with Promise, Peril." Signal, November 1993, pp. 19-20.

Canavan, Gregory H. "Changing Times Implode Defense Science Dynamics." Signal, September 1993, pp. 49-50.

Chairman of the Joint Chiefs of Staff. Command and Control Warfare: Memorandum of Policy No. 30. Washington: 1993.

Charlton, James. The Military Quotation Book. New York: St. Martin's Press, 1990.

"Commanders Pull Intelligence in Information Warfare Strategy." Signal, August 1994, pp. 29-31.

Computers: Crimes, Clues and Controls. Washington: Prevention Committee, President's Council on Integrity and Efficiency, 1986.

"Copernicus Forward: C4I for the 21st Century." Surface Warfare, July/August 1995, pp. 2-7.

Eisen, Jr., Stefan. "Netwar, It's Not Just for Hackers Anymore." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Emmett, Peter C. "Software Warfare: the Militarization of Logic." Joint Force Quarterly, Summer 1994, pp. 84-90.

Evancoe, Paul and Mark Bentley. "CVW--Computer Virus as a Weapon." Military Technology, May 1994, pp. 38-40.

"EW Expands into Information Warfare." Aviation Week & Space Technology, 10 October, 1994, pp. 47-48.

Facsimile from Navy and Marine Corps Intelligence Training Center "Nodal Analysis," Dam Neck, VA. 17 January 1996.

FitzGerald, Mary C. "Russian Views on Information Warfare." Army, May 1994, pp. 54-60.

Geisenheyner, Stefan. "How Vulnerable are C3I Networks? Jamming Versus Intercept and Decryption." Armada International, June/July 1990, pp. 46-48+.

Gordon, Michael R. "Admiral with High-Tech Dreams Has Pentagon at War With Itself." The New York Times, 12 December 1994, pp. A1 & A17.

Grier, Peter. "Information Warfare." Air Force Magazine, March 1995, pp. 34-37.

_____. "The Data Weapon." Government Executive, June 1992, pp. 23-26.

Hutcherson, Norman B. "Command & Control Warfare--Putting Another Tool in the War-Fighter's Data Base." Published Research Paper, Maxwell Air Force Base, AL: Air University Press, September 1994.

"Information Dominance Edges Toward New Conflict Frontier." Signal, August 1994, pp. 37-40.

Jensen, Owen E. "Information Warfare: Principles of Third-Wave War." Airpower Journal, Winter 1994, pp. 35-43.

Joint Chiefs of Staff. Doctrine for Joint Operations: Joint Pub. 3-0. Washington: February, 1995.

Leahy, Kevin B. "Can Computers Penetrate the Fog of War?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994.

Leigher, William E. "The Revolution in Military Affairs and Information Warfare." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Libicki, Martin C. "What is Information Warfare?" Unpublished Paper, U.S. National Defense University, Washington: 1995.

Lind, William S., Keith M. Nightengale, Scott Schmitt, Joseph W. Sutton, and G.I. Wilson. "The Changing Face of War into the Fourth Generation." Military Review, October 1989, p. 211.

Luoma, William M. "The Computer Virus: Weapon of Mass Destruction?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994.

_____. "Netwar: The Other Side of Information Warfare." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994.

Macedonia, Michael R. "Information Technology in Desert Storm." Military Review, October 1992, pp. 34-41.

Matthews, William. "Girding for Cyberwar." Army Times, 18 July 1994, p. 36.

_____. "School is in for 'Information Warfare'." Army Times, 23 May 1994, p. 28.

_____. "Susceptible to Sabotage: 'Weapons of Preference' are Vulnerable." Navy Times, 5 February 1996, p. 28.

Metzgar, Terry. "Hostile Intercepts Aimed at Information Systems." National Defense, May/June 1993, pp. 24-26.

Oder, Joseph E. "Digitizing the Battlefield: The Army's First Step to Force XXI." Army, May 1994, pp. 37-38, 42.

Owens, Ira C. "Army Intelligence Operations in Force XXI." Army, October 1994, pp. 145-149.

Oxburgh, E.R. "Future Military Technology and the West." The RUSI Journal, December 1992, pp. 49-55.

Planning Considerations for Defensive Information Warfare: Information Assurance. Arlington, VA: Defense Information System Agency, 1993.

Powell, Colin L. "Information-Age Warriors." Byte, July 1992, p. 370.

Reitinger, Kurt C. "Command and Control for Third Wave Warfare." Army, February 1995, pp. 9-14.

Robinson, Clarence A. "Software Security Protects Workstations, Laptop Data." Signal, October 1994, pp. 19-22.

Rowe, Wayne J. Information Warfare: a Primer for Navy Personnel. Strategic Research Department Research Report 6-95. Newport, RI: U. S. Naval War College. Center for Naval Warfare Studies. Strategic Research Department, 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder Mountain Press, 1994.

Scott, William B. " 'Information Warfare' Demands New Approach." Aviation Week & Space Technology, 13 March 1995, pp. 85-88.

Sexton, Joanne. "A Combatant Commander's Organizational View of Information Warfare and Command and Control Warfare." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Smith, Jr., Edward A. "Putting it Through the Right Window." U.S. Naval Institute Proceedings, June 1995, pp. 38-40.

Toffler, Alvin and Heidi. War and Anti-War. New York: Bantam Books, 1993.

U.S. Dept. of the Air Force. Cornerstones of Information Warfare. Washington: 1995.

U.S. Dept. of Defense. Defensive Information Warfare Strategy. Draft, Washington: 1995.

U.S. Dept. of Defense. Information Warfare. Draft, Washington: April 1995, pp. 1-3.

Waller, Douglas. "Onward Cyber Soldiers." Time, 21 August 1995, pp. 38-44.